The Human Factor in Cybersecurity

Name: Daisy Gonzalez

Date: February 27, 2022

Details

In a scenario where my budget is limited and I had to balance the tradeoff of training and additional technology, I would prioritize training over additional technology. Humans are a major point of failure in a cybersecurity program, in the same way that a strong cybersecurity program relies heavily on humans.

Many vulnerabilities and threats are initiated by humans. There have been many cases where employees have shared critical information with unauthorized parties, intentionally and unintentionally (Capone, 2018). And over 90% of successful breaches worldwide began with phishing emails (cyberbitsetc.org), a type of social engineering attack that relies on human involvement. I believe that many of these mistakes can be mitigated with proper training. In my program I would implement a human-centered approach by applying behavioral science in my research and training designs. My approach would ultimately mirror that of Pfleeger et al (2012), who states that “if humans using computer systems are given the tools and information they need, taught the meaning of responsible use, and then trusted to behave appropriately with respect to cyber security, desired outcomes may be obtained…[p 5]. Our network systems would not exists without humans so who better to protect these systems than humans themselves. It is important to recognize that a strong cybersecurity program cannot depend on human alone. Let's use the log of an intrusion prevention/detection system for example. This type of system cannot work without both the system and a human doing its job. IPS/IDS are a great way to better protect your system and thwart potential attacks, but they aren’t 100% reliable and are prone to experience false positives and false negatives. If humans are properly trained, they’ll know and be trusted to regularly review their logs so that they can omit false positives and check for false negatives. Both proper training and the technology you’re using is important, but the tech would be almost useless without properly trained employees.

References

Pfleeger, S., et al. (2012). *Leveraging Behavioral Science to Mitigate Cyber Security Risk*. MITRE. https://www.mitre.org/sites/default/files/pdf/12_0499.pdf

Capone, J. (2018). *The Impact of Human Behavior on Security*. CSO. https://www.csoonline.com/article/3275930/the-impact-of-human-behavior-on-security.html

Cybersecurity as a Behavioral Science: Part 1. CyberBitsEtc. *https://www.cyberbitsetc.org/post/cybersecurity-as-a-behavioural-science-part-1*